AO 106 (Rev. 04/10) Application for a Search Warrant

AUTHORIZED AND APPROVED/DATE: _____

UNITED STATES DISTRICT COURT

for the

Western District of Oklahoma

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

ELECTRONIC DEVICES: A blue Apple iPhone in a gray case, IMEI Unknown, a gray Apple iPad in a gray and clear case IMEI Unknown, a Dell Optiplex 5070 tower SN#ZZ45P23, and a Dell D05D tower SN# SN: HTBN213737

Case No. M-24-844-STE

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, which is incorporated by reference herein.

located in the Western District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252A(a)(5)(B), 2252A(a)(2), 2251(a), 1153, and 2243(a)	Possessing and Accessing Material with the Intent to View Child Pornography, Receipt of Child Pornography, Distribution of Child Pornography, and Sexual Abuse of a Minor in Indian Country

The application is based on these facts:

See Affidavit of FBI SA Paige Lang, which is attached and incorporated by reference herein.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Paige Lang, Special Agent FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: Nov 15, 2024

Judge's signature

City and state: Oklahoma City, Oklahoma

Shon T. Erwin, U.S. MAGISTRATE JUDGE
Printed name and title

THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF ELECTRONIC DEVICES: A BLUE APPLE IPHONE IN A GRAY CASE, IMEI UNKNOWN, A GRAY APPLE IPAD IN A GRAY AND CLEAR CASE IMEI UNKNOWN, A DELL OPTIPLEX 5070 TOWER SN#ZZ45P23, AND A DELL D05D TOWER SN# SN: HTBN213737	Case No. _____ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Paige Lang, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation and have been since February of 2022. During my training and since that time, I have received formal training from the FBI as well as training through contact with experts from various law enforcement agencies regarding a wide range of criminal offenses. Based on my training and experience relating to the investigation of child pornography and based upon interviews I have conducted with other officers, defendants, informants, and other witnesses and participants in child exploitation, I am familiar with the ways that child pornography is manufactured and distributed. My familiarity includes the various means and methods by which producers of child pornography manufacture and distribute pornography by using cellular smartphones.

2. As a Special Agent with the FBI, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

3. The information contained in this affidavit is based upon my personal knowledge and observation, my training and experience, conversations with other law enforcement officers

and witnesses, and review of documents and records. This affidavit is made in support of an application for a warrant to search the one blue Apple iPhone with gray case (DEVICE 1), one gray Apple iPad with gray and clear case (DEVICE 2), one Dell Optiplex 5070 tower SN: ZZ45P23 (DEVICE 3), and one Dell D05D tower SN: HTBN213737 (DEVICE 4) (hereinafter referred to as the "SUBJECT DEVICES"). The SUBJECT DEVICES are described in detail in Attachment A to this affidavit. I request a warrant to search the SUBJECT DEVICES for the items specified in Attachment B hereto, which constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. § 2252A(a)(5)(B) (possessing and accessing with intent to view material containing child pornography), 18 U.S.C. § 2252A(a)(2)(A) (receipt of child pornography), 18 U.S.C. § 2251(a) (production of child pornography), and 18 U.S.C. §§ 1153 and 2243(a) (sexual abuse of a minor in Indian Country).

4. This investigation, described more fully below, has revealed that an individual knowingly utilized and accessed the SUBJECT DEVICES to violate the foregoing statutes, and that there is probable cause to believe that evidence, fruits, and instrumentalities of such violations are located on the SUBJECT DEVICES.

5. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me regarding this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to support the issuance of a search warrant.

TERMS

6. Based on my training and experience, I use the following technical terms and definitions:

a. "Computer," as used broadly herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or

storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones. *See* 18 U.S.C. § 1030(e)(1).

b. A provider of "Electronic Communication Service" ("ESP"), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

c. "Short Message Service" ("SMS"), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone.

d. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178).

e. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

f. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

g. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

h. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

i. "Cloud storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet.

CHARACTERISTICS COMMON TO INDIVIDUALS WITH INTENT TO COLLECT, RECEIVE, OR DISTRIBUTE CHILD PORNOGRAPHY

7. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals with intent to view and/or possess, collect, receive, or distribute images of child pornography:

a. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain photos, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals with intent to view and/or possess, collect, receive, or distribute pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography also may correspond with and/or meet others to share information and

materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who would have knowledge about how to access online forums, such as bulletin boards, newsgroups, internet relay chat or chat rooms are considered more advanced users and therefore more experienced in acquiring and storing a collection of child pornography images.

8. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND ON DIGITAL MEDIA STORAGE DEVICES AND CHILD PORNOGRAPHY

9. The ability of a smartphone to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media used in smartphones has grown tremendously within the last several years. These storage devices can store thousands of images at very high resolution. Given the storage capabilities, modern cellular phones can retain many years' worth of a user's data, stored indefinitely. Even deleted data can often be forensically recovered.

10. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos

and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

11. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

12. As is the case with most digital technology, communications by way of smartphone can be saved on the device. Storing this information can be intentional, i.e., by saving an email as a file on the smartphone or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data. Further, even if deleted, forensic examination can sometimes recover files and data including deleted picture files. I know that smartphones can be forensically examined, and forensic analysts can learn much detail about the user's habits and online activities, including websites visited, files downloaded, Google searches performed, locations where the device was used, dominion and control information, etc.

13. Smartphones can store the equivalent of thousands of pages of digital information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires the searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks depending on the volume of the data stored, and it would be generally impossible to accomplish this kind of data search on site.

BACKGROUND OF INVESTIGATION

14. On October 14, 2024, Newcastle Police Department (NPD) received a report of alleged sexual assault of a minor and child pornography production. Thirteen-year-old, Jane Doe, disclosed to her mother that their neighbor, seventy-six-year-old, DONALD GENE JOHNSON, touched her inappropriately and gave her money to provide pornographic images of herself to him via text message. Jane Doe's mother provided NPD with Jane Doe's cell phone, which was purchased by JOHNSON. Jane Doe's mother signed a consent to search the cell phone.

15. Law Enforcement reviewed an extraction of Jane Doe's phone. JOHNSON was listed as "Don" in Jane Doe's contacts with cell phone number (405) 210-0708. A string of text messages was identified between Jane Doe and JOHNSON. The text messages ranged from October 8, 2024, to October 9, 2024. JOHNSON sent a text message to Jane Doe which stated, "I'm sorry too. Since you didn't text me any all evening I assumed you were through with me and I went back to Gracie". Jane Doe responded and asked if Gracie and JOHNSON were back together. JOHNSON told Jane Doe, "You really need to put that phone on another account", "I'm returning the new phone along with the SHEIN order" and "I warned you". A few text messages are exchanged where Jane Doe explains why she did not respond back to JOHNSON. JOHNSON told Jane Doe, "Well, I did the unforgivable, I fucked Gracie, not because I wanted to, because I wanted to get you out of my mind".

16. JOHNSON tells Jane Doe, "[…] you don't even like me to touch you or kiss you the way we used to. Is that what you call love?" JOHNSON later stated, "Still doesn't explain why you don't want me to touch you or kiss you like before. Especially when you were doing it with Justin". Jane Doe apologized to JOHNSON. JOHNSON stated, "I don't want you to fuck me, I understand that. But the other things I want you won't do". Jane Doe confirmed she would do what JOHNSON wanted. JOHNSON asked, "The kissing and touching?" Jane Doe confirmed. JOHNSON asked, "Are you sure?" Jane Doe confirmed. JOHNSON stated, "I will give us one more chance".

17. Later in the text thread, Jane Doe asked, "Can we go get a pizza". JOHNSON replied, "If you love me". Jane Doe stated, "Ok we r coming and I do lol" and "Can we get a drink first". JOHNSON asked, "Are you part of this relationship?" Jane Doe confirmed and later asked for an item from Walmart. JOHNSON replied, "Ok" and "I really need that pic". They continued to text about what Jane Doe purchased at Walmart. JOHNSON stated, "And the pic, plzzzz". Jane Doe responded, "Ok". JOHNSON sent, "2", "1 open 1 closed", and "and one of your top". Jane Doe responded, "Okay". JOHNSON messaged, "Delete this" and "Thanks".

18. Jane Doe then asked JOHNSON for five hundred dollars to help her mother with rent. JOHNSON agreed to give Jane Doe the money and they exchanged multiple text messages about the money. Jane Doe sent to JOHNSON, "I sent u smt so u owe me". JOHNSON replied, "I have paid for that with the 500 you spent already this week". Their conversation continued about the five hundred dollars.

19. Throughout the text message exchange between Jane Doe and JOHNSON, JOHNSON threatened to turn off Jane Doe's phone, take away items he purchased for her, and accused Jane Doe of cheating on him. When Jane Doe complied with JOHNSON's requests, he would provide her with additional items.

20. On October 30, 2024, a child forensic interview was conducted at the Mary Abbott house with Jane Doe. She disclosed that JOHNSON was her neighbor. Jane Doe would help him put away his groceries and take care of his yard. JOHNSON paid Jane Doe twenty dollars for her help. July 2024 was the first time Jane Doe remembered JOHNSON touching her. Jane Doe remembered it was in July because she stayed with her uncle and came home at the end of June beginning of July. She was sitting on JOHNSON's couch. JOHNSON was ordering Little Caeser's and asked Jane Doe to come order her food. Jane Doe walked over to JOHNSON and stood in front of his recliner where JOHNSON was sitting. JOHNSON put his hand down the front of her pants, under her underwear, and rubbed "the top." Jane Doe stated it felt weird. JOHNSON stopped and Jane Doe went home.

21. Jane Doe recalled another time JOHNSON touched her. They were on their way back home from Walmart. She stated JOHNSON pulled over on the side of the road and slid his hand down the front of Jane Doe's shirt. JOHNSON pulled Jane Doe's bra down in the middle and grabbed and squeeze her "boobs." Jane Doe stated it felt weird, and she asked JOHNSON what he was doing, but he did not answer. He stopped, and JOHNSON dropped Jane Doe off at her house. Jane Doe unloaded the groceries JOHNSON purchased for her and her family.

22. Jane Doe recalled the last time JOHNSON touched her. It was inside JOHNSON's house approximately a month ago (September 2024). Jane Doe sated she was sitting on JOHNSON's couch on the right side, and JOHNSON was sitting in the recliner. JOHNSON got up and sat in the middle of the couch next to Jane Doe. She recalled JOHNSON slid his hand down the front of her pants, under her underwear, and rubbed "the top." Jane Doe recalled JOHNSON used his middle finger to rub her, because she could feel the rest of his fingers touching her as well. Jane Doe stated he stopped, and she left the house. Jane Doe was shown a basic drawing of the front and back of a female and was asked to color in the area's where JOHNSON had touched

her. Jane Doe colored the breast and vagina area of the drawing. Jane Doe pointed to the vagina area, as the area she referenced as "the top." Jane Doe stated she only used that area to go to the bathroom.

23. During the forensic interview of Jane Doe, she disclosed that JOHNSON purchased Jane Doe an HMD-brand vibe phone and asked Jane Doe to send photographs of herself. Jane Doe sent JOHNSON photos of her breast with her bra and top pulled up, and photos of her vagina with her underwear pulled down. JOHNSON paid Jane Doe forty to sixty dollars for the photographs. Jane Doe stated she would communicate with JOHNSON through text message and send the photographs through text message. Jane Doe described JOHNSON's phone as a black iPhone with a gray and brown phone case.

24. On November 5, 2024, NPD executed a State of Oklahoma search warrant at JOHNSON's residence located at 200 Naomi Lane #1, Newcastle, Oklahoma. During the execution of the search the SUBJECT DEVICES were seized.

25. In my training and experience, it is common for Apple users to have their Apple devices connected to an iCloud account. Users can access their iCloud account from non-apple devices and retrieve their stored content from cloud storage.

26. On November 6, 2024, a probable cause affidavit was signed in the District Court of Chickasaw Nation for the arrest of JOHNSON. JOHNSON is a member of the Chickasaw Nation and the acts described herein occurred within the jurisdictional boundaries of the Chickasaw Nation.

SPECIFICS OF SEARCH AND SEIZURE OF CELL PHONES

27. Searches and seizures of evidence from smartphones commonly require agents to download or copy information from the smartphones and its components, such as a flash drive or

other digital storage units attached to the phone, to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true for the following two reasons:

a. Smartphone devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all of the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching smartphones for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of smartphone hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a smartphone system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since smartphone evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

28. In order to fully retrieve data from a smartphone system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child exploitation where the evidence frequently includes graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition,

the analyst needs all of the system software (operating systems or interfaces, and hardware drivers) and any application software which may have been used to create the data (whether stored on hard drives or on external media).

29. Furthermore, because there is probable cause to believe that the smartphone and its storage devices are all instrumentalities of crimes they should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED REGARDING ELECTRONIC DATA

30. The search procedure for electronic data contained in smartphone hardware, smartphone software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. on-site triage of smartphone systems to determine what, if any, storage devices or digital storage units have been connected to such smartphone systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

b. on-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;

c. examination of all of the data contained in such smartphone hardware, smartphone software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

d. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth

herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offense, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offense specified above);

e. surveying various file directories and the individual files they contain;

f. opening files in order to determine their contents;

g. scanning storage areas;

h. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

i. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

SMARTPHONES

31. Finally, based on my training and experience, I know that people who use their smartphone to view/access/possess child pornography do so in private to avoid detection. I believe there is probable cause that the SUBJECT DEVICES and other digital file storage device(s) attached to the SUBJECT DEVICES will contain evidence of the aforementioned criminal violations, as set forth in detain in Attachment B.

CONCLUSION

32. Based on the above information, there is probable cause to believe that the foregoing laws have been violated, and that the following property, evidence, fruits, and instrumentalities of these offenses are located on the SUBJECT DEVICES.

33. Based upon the foregoing, I respectfully request that this Court issue a search warrant for the SUBJECT DEVICES, described in Attachment A, authorizing the seizure of the items described in Attachment B to this affidavit.

Paige Lang
Special Agent
Federal Bureau of Investigation

SUBSCRIBED AND SWORN to before me this 15th day of November, 2024.

Shon T. Erwin
SHON T. ERWIN
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF DEVICE 1
One blue Apple iPhone with gray case

DESCRIPTION OF DEVICE 2
One gray Apple iPad with gray and clear case

DESCRIPTION OF DEVICE 3
One Dell Optiplex 5070 tower SN: ZZ45P23

DESCRIPTION OF DEVICE 4
One Dell D05D tower SN: HTBN213737

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Smartphone(s), as broadly defined in 18 U.S.C. § 1030(e), other digital file storage devices, smartphone hardware, smartphone software, smartphone that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography.

2. All fruits, instrumentalities, and evidence, in any format or medium, of violations of 18 U.S.C. § 2252A's enumerated offenses.

3. All child pornography.